GALOIS GROUPS AND AN OBSTRUCTION TO PRINCIPAL GRAPHS OF SUBFACTORS

MARTA ASAEDA

Abstract. The Galois group of the minimal polymonal of a Jones index value gives a new type of obstruction to a principal graph, thanks to a recent result of P.Etingof, D.Nikshych, and V.Ostrik. We show that the sequence of the graphs given by Haagerup as candidates of principal graphs of subfactors, are not realized as principal graphs for $7 < n \leq 27$ using GAP program. We further utilize Mathematica to extend the statement to $27 < n \leq 55$. We conjecture that none of the graphs are principal graphs for all $n > 7$, and give an evidence using Mathematica for smaller graphs among them for $n > 55$. The problem for the case $n = 7$ remains open, however, it is highly likely that it would be realized as a principal graph, thanks to numerical computation by Ikeda.

1. Introduction

Since V. F. R. Jones introduced the index theory of subfactors in [15], the theory of operator algebras have been achieving a remarkable development, having relations with low dimensional topology, solvable lattice model theory, conformal field theory and quantum groups. The following was the first breakthrough in the theory of Jones. For a subfactor $N \subset M$, the index value $[M : N]$ belongs to the set

$$\{4\cos^2\frac{\pi}{n}|\ n = 3, 4, 5\cdots\} \cup [4, \infty].$$

Later, he also introduced a principal graph and a dual principal graph as finer invariants of subfactors. The Perron-Frobenius eigenvalue of the (dual) principal graph of a finite-depth subfactor $N \subset M$ is equal to $\sqrt{[M : N]}$. Using this fact Jones proved in the middle of 1980's that subfactors with index less than 4 have one of the Dynkin diagrams of ADE type as their (dual) principal graphs. A. Ocneanu discovered a complete invariant for finite depth subfactors called "paragroup" and announced in [21] that subfactors with index less than 4 are completely classified by the Dynkin diagrams A_n, D_{2n}, E_6, and E_8. (See also [2], [12], [14], [16], [23].) Ocneanu's invariant consists of numerical data

The authors were sponsored in part by NSF grant #DMS-0504199.

called biunitary connection which is defined on squad of four graphs as depicted below: where Perron-Frobenius eigenvalues (PFEVs) of $\mathcal{G}$

$$\begin{tikzcd} V_0 \arrow[r, no head, "\mathcal{G}"] \arrow[d, no head, "\mathcal{G}"'] \arrow[dr, phantom, "\alpha"] & V_1 \arrow[d, no head, "\mathcal{H}"] \\ V_2 \arrow[r, no head, "\mathcal{H}"'] & V_3 \end{tikzcd}$$

FIGURE 1. the biunitary connection α with four graphs

and $\mathcal{H}$ coinside. When a biunitary connection satisfies an axiom called *flatness*, it is called a paragroup. Completeness of paragroups as invariants of subfactors is proved by S.Popa in [22]. In such case the graphs $\mathcal{G}$, $\mathcal{H}$ which are used to define a biunitary connection turns out to be the (dual) principal graph of the subfactor. Moreover each vertex of the graphs corresponds to a bimodule generated by the subfactor, and that the (dual) principal graph encodes the fusion rule of the bimodules. Therefore, the problem of whether a given pair of graphs are realized as (dual) principal graph is reduced to construction of biunitary connection and to prove that it is flat. The detail of the paragroup theory is found in [5].

After that, Popa ([22]) extended the correspondance between paragroups and subfactors of the hyperfinite II_1 factor to the strongly amenable case, and gave a classification of subfactors with index equal to 4. (In this case, the dual principal graph of a subfactor is the same as the principal graph. See also [13].) Some subfactors with index larger than 4 had been constructed from other mathematical objects. For example, we can construct a subfactor from an arbitrary finite group by a crossed product with an outer action, and this subfactor has an index equal to the order of the original finite group. Trivially, the index is at least 5 if it is larger than 4. We also have subfactors constructed from quantum groups $U_q(sl(n))$, $q = e^{2\pi i/k}$ with index $\frac{\sin^2(n\pi/k)}{\sin^2(\pi/k)}$ as in [26] and these index values do not fall in the interval $(4, 5)$. A subfactor with an index $3+\sqrt{3} = 4.73...$ appeared in [7] is constructed by embedding the graph algebra of A_{11} into that of E_6. U.Haagerup gave in 1991 a list of possible candidates of graphs which might be realized as (dual) principal graphs of subfactors with index in $(4, 3+\sqrt{3}) = (4, 4.732\cdots)$ in [8]. We see three pairs of finite graphs, including two pairs with parameters, along with a pair of infinite graphs A_∞ in (1), in §7 of [8]. Since then D. Bisch proved that a subfactor with (dual) principal graph (4) in §7 of [8] does *not* exist [3] by checking inconsistency of

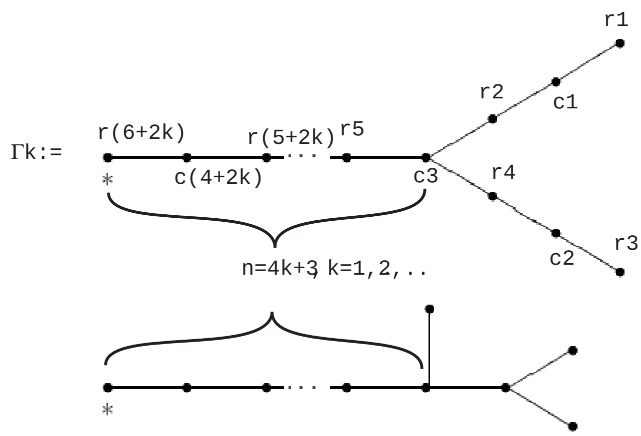

FIGURE 2. The the pairs of graphs (2) in the list of Haagerup

fusion rule on the graph. Haagerup and the author proved that two pairs of graphs: the case $n = 3$ of (2): see Figure 2 as well as the case (3) in §7 of [8], are realized as (dual) principal graphs of subfactors, and that such subfactors are unique respectively ([1]). The remaining problem was whether the graphs for the case $n > 3$ of (2) as in Figure 2 would be realized as (dual) principal graphs of subfactors. Haagerup proved that the obstruction as found for the case (4) by Bisch does not exist on any of the pairs of the graph in (2). Moreover he proved that unique biunitary connection exists for each the pair of the graphs ([9]). For the case $n = 7$, it was numerically checked by K.Ikeda that the biunitary connection is flat([11]). There has been no progress for several years since then. Recently P.Etingof, D.Nikshych, and V.Ostrik showed in [4] Theorem 8.51, that the index of a subfactor has to be a cyclotomic integer, namely an algebraic integer that lies in a cyclotomic field. This implies that if the square of PFEV of a graph is not a cyclotomic integer, the graph cannot be the (dual) principal graph of a subfactor.

In this paper we prove that the graphs in Figure 2 are not (dual) principal graph for $n = 4k + 3$ for $1 < k \leq 13$ by computing Galois groups of minimal polynomials of the square of PFEV of the graphs. We also prove that for the case $k = 1$ the square of PFEV of the graphs is a cyclotomic integer: thus we cannot eliminate the possibility that the graphs might be (dual) principal graphs of a subfactor. We further give an evidence by Mathematica computation that the graphs for larger k are not principal graphs. We conjecture that for the case $k > 1$ none of the graph is (dual) principal graph of a subfactor.

The author is much grateful to Y. Kawahigashi, D.Bisch, and V.Jones for informing me of the result in [4] and suggesting the possibility of utilizing Galois theory. She also thanks U.Haagerup for sharing with me his unpublished results on the larger graphs, and L.Washington, T.Saito for helpful discussion on Galois theory.

2. Preliminaries

In the following we list some known theorems in Galois theory necessary for later discussion.

Theorem 2.1. *(Galois correspondence* [10]*)*
Let F be a finite dimensional Galois extension of K. Then there is one-to-one correspondence between the set of all intermediate fields of the extension and the set of all subgroups of the Galois group $G = \mathrm{Aut}_K F$, given by $E \mapsto \mathrm{Aut}_E F$. An intermediate field E is Galois over K if and only if $\mathrm{Aut}_E F$ is a normal subgroup of G. In this case $Aut_K E \cong G/\mathrm{Aut}_E F$.

Theorem 2.2. *(Kronecker-Weber,* [25]*)*
Let E be an extension of $\mathbb{Q}$ so that $Aut_{\mathbb{Q}} E$ is abelian. Then the field E is a subfield of a cyclotomic field, that is, a field extension of $\mathbb{Q}$ by a primitive root of unity.

Theorem 2.3. *(*[20]*) Let $p(x) \in \mathbb{Q}[x]$ be a monic irreducible polynomial of degree n, and let G be its Galois group. Let $\xi_1, ...\xi_n$ be the roots of p. We define the discriminant of p by $D_p = {\Delta_p}^2$, where*

$$\Delta_p = \prod_{i<j}(\xi_i - \xi_j)$$

up to sign. Then we have

$${\Delta_p}^2 \in \mathbb{Q},$$

and

$$G \subset \mathfrak{A}_n \Longleftrightarrow \Delta_p \in \mathbb{Q}.$$

We may replace $\mathbb{Q}$ by $\mathbb{Z}$ if $p(x) \in \mathbb{Z}[x]$.

Remark 2.4. *(*[24]*, §26-28) The discriminant D_p of a monic polynomial $p(x)$ relates to the resultant $Res(p, p')$ of p and p' by $D_p = (-1)^{n(n-1)}\mathrm{Res}(p, p')$. (Note that in* [24] *the sign is omitted.) The resultant $Res(p, p')$ is given as follows: Let $p(x) = x^n + a_{n-1}x^{n-1} + ...a_1x + a_0$.*

Then the resultant $Res(p,p')$ is equal to

$$\begin{vmatrix} 1 & a_{n-1} & a_{n-2} & \cdots & \cdots & a_0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & a_{n-1} & a_{n-2} & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 & a_{n-1} & a_{n-2} & \cdots & \cdots & a_0 \\ n & b_{n-1} & b_{n-2} & \cdots & \cdots & b_0 & 0 & \cdots & 0 & 0 \\ 0 & n & b_{n-1} & b_{n-2} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & n & b_{n-1} & b_{n-2} & \cdots & \cdots & b_0 \end{vmatrix},$$

where $b_i := ia_i$. It is easily obtained that $D_p = (-1)^c|D_p|$, where c is half the number of complex roots of $p(x)$.

Our use of these theorems are as follows: Let d be an algebraic integer with the minimal polynomial $p(x) \in \mathbb{Z}[x]$. Suppose d lies in a cyclotomic field F. Then $\mathbb{Q}(d)$ is an intermediate field of $F/\mathbb{Q}$. Thus by Galois correspondence it corresponds to a subgroup of $\mathrm{Aut}_{\mathbb{Q}}F = \mathbb{Z}_n$ for some n. Since any subgroup of $\mathbb{Z}_n$ is normal, the extension $\mathbb{Q}(d)/\mathbb{Q}$ is Galois. Thus all the roots of $p(x)$ belong to $\mathbb{Q}(d)$, and the Galois group of $p(x)$ is a quotient of $\mathbb{Z}_n$, which is always abelian. Together with Kronecker's theorem, we conclude the following:

Proposition 2.5. *An algebraic number d is a cyclotomic integer if and only if its minimal polynomial has an abelian Galois group.*

The following facts are useful in computing Galois group.

Proposition 2.6. *([20]) Let K be a field, $f(x) \in K[x]$, and E be a splitting field of f generated by its roots over K. If f is irreducible and separable,* $\mathrm{Gal}(E/K) = \mathrm{Gal}(f)$ *acts transitively on the roots of f, i.e.* $\mathrm{Gal}(f)$ *is a transitive subgroup of $\mathfrak{S}_n$, where $n = \deg f$. Furthermore* $|\mathrm{Gal}(f)|$ *is divisible by n.*

3. Minimal polynomials for the square of Perron-Frobenius eigenvalues

In this section we give a formula for the polynomials which are candidates for minimal polynomials of the square of PFEVs of the graphs in Figure 2. Since PDEVs of each pair coincide, we only use the first sequence of the graphs. The adjacency matrix of the graph Γ_k is as

follows:

$$A_k := \begin{array}{c} \\ r_1 \\ r_2 \\ r_3 \\ r_4 \\ r_5 \\ \vdots \\ r_{5+2k} \\ r_{6+2k} \end{array} \begin{array}{c} \begin{array}{ccccccc} c_1 & c_2 & c_3 & c_4 & \cdots & \cdots & c_{4+2k} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 1 & 0 & \cdots & \cdots & 0 \\ \vdots & 0 & 1 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 1 & 0 \\ 0 & 0 & \cdots & \cdots & 0 & 1 & 1 \end{pmatrix} \end{array},$$

Where (i, j)-entry is given by the number of edges connecting r_i and c_j. Notice that r_i's are even vertices and c_j's are odd vertices of the graph Γ_k, considering $*$ as zero-th vertex. The PFEV β_k is the unique eivenvalue of the matrix

$$M_k := \begin{bmatrix} \mathbf{0}_{6+2k} & A_k \\ {A_k}^t & \mathbf{0}_{4+2k} \end{bmatrix}$$

with the largest norm. Note that the rows (resp. columns) of M_k are labeled by the vertices of Γ_k in the order of $r_1, r_2, ..., r_{6+2k}, c_1, ..., c_{4+2k}$. It is known that β_k is a real number, its eigenspace is one dimensional, and an eigenvector can be taken to be a real vector. Let u_k be the eigenvector chosen so that the entry corresponding to the row labeled by r_{6+2k} will be one. We may regard u_k as a direct sum of two vectors $u_k = (v_k, w_k)$, where v_k consists of the entries corresponding to even vertices (i.e. r's), w_k corresponds to odd vertices (i.e. c's). Then we have the following relation:

$$\begin{aligned} A_k w_k &= \beta_k v_k, \\ (A_k)^t v_k &= \beta_k w_k. \end{aligned}$$

Consider

$$(M_k)^2 = \begin{bmatrix} A_k {A_k}^t & \mathbf{0} \\ \mathbf{0} & {A_k}^t A_k \end{bmatrix}.$$

The largest norm of the eigenvalues is given by ${\beta_k}^2 =: d_k$. On the other hand clearly d_k is an eigenvalue with eivenvector u_k, thus d_k is the PFEV of $(M_k)^2$. Since non-zero eigenvalues of $A_k {A_k}^t$ and that of ${A_k}^t A_k$ coincides, d_k must be the PFEV of ${A_k}^t A_k$ (resp. $A_k {A_k}^t$). Thus we deal with $N_k := {A_k}^t A_k$, since it is a smaller matrix. N_k is given as

follows:

$$N_k = \begin{array}{cc}
 & \begin{array}{ccccccccc} c_1 & c_2 & c_3 & c_4 & \cdots & \cdots & \cdots & c_{3+2k} & c_{4+2k} \end{array} \\
\begin{array}{c} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ \vdots \\ c_{4+2(k-1)} \\ c_{3+2k} \\ c_{4+2k} \end{array} &
\begin{pmatrix}
2 & 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 2 & 1 & 0 & & & & & \vdots \\
1 & 1 & 3 & 1 & 0 & & & & \vdots \\
0 & 0 & 1 & 2 & 1 & 0 & & & \vdots \\
0 & 0 & 0 & 1 & 2 & 1 & 0 & & \vdots \\
\vdots & & & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\
\vdots & & & & 0 & 1 & 2 & 1 & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 2 & 1 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 2
\end{pmatrix}
\end{array}$$

Let us call the $(3+2k)\times(3+2k)$ submatrix of N_k containing first $3+2k$ columns and rows $N_{k-1/2}$. Let p_k be the characteristic polynomial of N_k. Then clearly for every half integer $k > 1$ we have the following recursive relation:

$$p_k(x) = (2-x)p_{k-1/2}(x) - p_{k-1}(x),$$

and from this we easily get

$$\begin{aligned}
p_k(x) &= (x^2-4x+2)p_{k-1}(x) - p_{k-2}, \\
p_0(x) &= (x^2-5x+3)(x-2)^2, \\
p_1(x) &= (x^3-8x^2+17x-5)(x-2)^2(x-1).
\end{aligned}$$

Since both p_0 and p_1 contain $(x-2)^2$ as factor, $p_k(x)$ for any k also contains $(x-2)^2$. Since our concern is minimal polynomials for PFEVs, we set $q_k(x) := p_k(x)/(x-2)^2$. Obviously $q_k(x)$ satisfy the same recursive equation. Furthermore we have the following:

Proposition 3.1. *The polynomial $q_k(x)$ is divisible by $(x-1)$ if and only if $k \equiv 1$ mod 3.*

Proof
We simply plug in $x = 1$ in the equation: we know that $q_0(1) = -1$, $q_1(1) = 0$, and we easily obtain $q_2(1) = 1$. Suppose $q_{k-2}(1) = 0$ Then $q_k(1) = -q_{k-1}(1)$, thus $q_{k+1}(1) = -q_k(1) - q_{k-1}(1) = 0$, i.e. $q_{k+1}(x)$ is divisible by $(x-1)$ in this case. Suppose $q_{k-2}(1) = \pm 1$. Then $q_k(1) = -q_{k-1}(1) \mp 1$, thus $q_{k+1}(1) = -q_k(1) - q_{k-1}(1) = \pm 1$. □

We may solve the recursive equation explicitly in a standard method: we obtain the following:

$$q_k(x) = A(x)a(x)^{2k} + B(x)b(x)^{2k},$$

where $a(x) = (2-x+\sqrt{x^2-4x})/2$, $b(x) = (2-x-\sqrt{x^2-4x})/2$, $A(x) = \frac{-1}{a(x)^2-b(x)^2}(q_0(x)b(x)^2-q_1(x))$, and $B(x) = \frac{1}{a(x)^2-b(x)^2}(q_0(x)a(x)^2-q_1(x))$. We conjecture the following:

Conjecture 3.2. *Let*

$$r_k(x) = \begin{cases} q_k(x)/(x-1), & \text{if } k \equiv 1 \bmod 3, \\ q_k(x), & \text{else.} \end{cases}$$

Then $r_k(x)$ is irreducible for any k.

This is proved for the values of k up to 6 by using GAP [6]. (For $k = 0, 1$ it is obvious.) GAP is an open-source program designed for mathematicians that does not give any approximate solutions without an message stating so or deliberately set by each user to give an approximation, i.e. any solutions given by GAP is mathematically accurate at least to the level of published results. For larger k, it is checked by Mathematica for individual case. Mathematica is not an open-source software, and the users have no way of knowing the reliability of results, thus we do not dare to claim it as a proof. However we would like to note that we found a prime number for each k modulo which Mathematica thinks that $r_k(x)$ is irreducible, for $k = 7, ..., 13$. Following is the list of the smallest primes p used for each k: we list as (k, p). (7,3), (8,2), (9,5), (10,3), (11,3), (12, 2), (13, 11).
Since factorization of a polynomial modulo prime is a finite process, we can conclude that $r_k(x)$'s for $k = 7, ..., 13$ are irreducible. And for $k = 14, ..., 19$, Mathematica thinks that $r_k(x)$'s are irreducible for whatever reason we do not know. Note that the number "19" is totally arbitrary: it does not mean that it is the maximum k that Mathematica could handle.

4. Galois groups of $r_k(x)$ and cyclotomicity of d_k.

Our aim is to check if d_k is cyclotomic number. Thus we need to compute the Galois group of its minimal polynomial $m_k(x)$. If $r_k(x)$ in the previous section is irreducible, it coincides with $m_k(x)$. Otherwise $m_k(x)$ factors $r_k(x)$. For $k = 0, 1$, we have the following:

Proposition 4.1.

$$\begin{aligned} \mathrm{Gal}(r_0(x)) &= \mathbb{Z}_2 \\ \mathrm{Gal}(r_1(x)) &= \mathbb{Z}_3, \end{aligned}$$

where for a polynomial $f \in \mathbb{Q}[x]$, we denote its Galois group by $Gal(f)$.

Proof
Using Proposition 2.6, we have $\mathrm{Gal}(r_0(x)) = \mathbb{Z}_2 = \mathfrak{S}_2$ and that $\mathrm{Gal}(r_1(x))$

is a transitive subgroup of $\mathfrak{S}_3$, i.e. $\mathfrak{A}_3 = \mathbb{Z}_3$ or $\mathfrak{S}_3$. Now, we compute the discriminant of $r_1(x) = x^3 - 8x^2 + 17x - 5$ using the formula given in Remark 2.4. We have the resultant $\mathrm{Res}(r_1, r_1') = -139$, thus $D_{r_1} = (-1)^{3 \cdot 2/2} \cdot (-169) = 13^2$. Therefore $\mathrm{Gal}(r_1(x)) = \mathbb{Z}_3$. □

The above result implies that d_0, d_1 are cyclotomic numbers by Theorem 2.2. For $k = 0$ in fact we had already known that d_0 is cyclotomic, since the graph Γ_0 in Figure 2 is realized a principal graph. For $k = 1$, this result implies that Γ_1 still has a chance of being a principal graph, but it needs to be checked by other methods.

We may still utilize GAP for small values of k.

Proposition 4.2. *For $k = 2, ..., 6$, $\mathrm{Gal}(r_k) = \mathfrak{S}_{n_k}$, where $n_k = \deg(r_k)$.*

This implies that d_k's for $k = 2, ..., 6$ are not cyclotomic, thus corresponding Γ_k's cannot be realized as principal graphs of subfactors. The readers may wish to check it on their own for small k, here we provide the first two polynomials: $r_2(x) = x^6 - 13x^5 + 63x^4 - 140x^3 + 142x^2 - 59x + 7$, $r_3(x) = x^8 - 17x^7 + 117x^6 - 418x^5 + 827x^4 - 898x^3 + 502x^2 - 124x + 9$.

For larger k, we may still work using Mathematica. We have the following very strong fact:

Proposition 4.3. *([18]) Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial with degree n. Then $\mathrm{Gal}(f) = \mathfrak{S}_n$ if the discriminant of f is square-free.*

This in particular implies the following:

Theorem 4.4. *Let Γ be a finite graph, and d_Γ be the square of PFEV of Γ, and let $m_\Gamma(x)$ its minimal polynomial with degree larger than 2. Then Γ is not realized as a principal graph of a subfactor if the discriminant of m_Γ is square-free.*

Mathematica does not have a command for discriminant, however it does have resultant, thus we may compute discriminant up to sign. Below we show the mathematica computations. *ired*$[k, x]$ corresponds to $r_{k-1}(x)$. D[*function*, x] is the derivative of a given function in x.

$$\begin{aligned} \mathrm{dd[k\_]} &:= \mathrm{Abs[Resultant[Simplify[ired[k,x]], D[Simplify[ired[k,x]], x], x]]} \\ &\quad \text{(discriminant of } r_{k+1}(x)\text{)up to sign)} \\ \mathrm{fd[k\_]} &:= \mathrm{FactorInteger[Abs[Resultant[Simplify[ired[k,x]],} \\ &\quad \mathrm{D[Simplify[ired[k,x]], x], x]]]} \quad \text{(find the factorization of dd[k])} \end{aligned}$$

The followings are the results: note again that the numbering is shifted by 1 from our paper. Since the computation gives integers as result,

we can take the computation to be accurate. Here $\{\{p, n_p\}, \{q, n_q\}, ...\}$ means that the given number is prime-factorized in the form of $p^{n_p} \cdot q^{n_q} \cdot .....$

fd[3] =

$\{\{1471, 1\}, \{5171, 1\}\}$

fd[4] =

$\{\{1097, 1\}, \{4261, 1\}, \{8677, 1\}\}$

fd[5] =

$\{\{281, 1\}, \{643, 1\}, \{31281527, 1\}\}$

fd[6] =

$\{\{192667, 1\}, \{47117433796403, 1\}\}$

fd[7] =

$\{\{3, 1\}, \{47, 1\}, \{3323, 1\}, \{3613, 1\}, \{7487, 1\}, \{22182696017, 1\}\}$

fd[8] =

$\{\{29, 1\}, \{1427, 1\}, \{11933, 1\}, \{35419, 1\}, \{595801, 1\}, \{7143737, 1\}\}$

fd[9] =

$\{\{769765583537031753607466863873613, 1\}\}$

fd[10] =

$\{\{31, 1\}, \{1625255809, 1\}, \{1226665686533457543318366623, 1\}\}$

fd[11] =

$\{\{230113699, 1\}, \{1990348035579493, 1\}, \{47658861361724611, 1\}\}$

fd[12] =

$\{\{119813, 1\}, \{23296847792041232351, 1\}, \{2859814819272301965311\,87, 1\}\}$

fd[13] =

$\{\{17761, 1\}, \{15894547, 1\}, \{202995484303, 1\},$

$\{993013213822241, 1\}, \{2155998286155473, 1\}\}$

fd[14] =

$\{\{745621, 1\}, \{21802562773909, 1\}, \{468985859471443, 1\},$

$\{66977888927782595508 91, 1\}\}$

fd[15] =

$\{\{41, 1\}, \{85503853, 1\}, \{525628115273, 1\},$

$\{26408938174586924096295973552030291503248 17, 1\}\}$

$\mathrm{fd}[16] =$
$\{\{3, 1\}, \{943618253, 1\}, \{93745696465972150179 11, 1\},$
$\{460880508744251153175035011605736265 93, 1\}\}$
$\mathrm{fd}[17] =$
$\{\{1487, 1\}, \{14737, 1\}, \{42895179574588531, 1\},$
$\{60223738686748239042955251921402367435105456 9169, 1\}\}$
$\mathrm{fd}[18] =$
$\{\{281, 1\}, \{619, 1\}, \{21149, 1\}, \{2454047, 1\}, \{27050115645481, 1\},$
$\{109185979881289, 1\}, \{43780709722667314881498749709041286 97, 1\}\}$
$\mathrm{fd}[19] =$
$\{\{408019, 1\}, \{1085473, 1\}, \{318567199174826396 23, 1\},$
$\{30882063734866254693924456664259293347328726428674245 21, 1\}\}$
$\mathrm{fd}[20] =$
$\{\{29, 1\}, \{4783, 1\}, \{4700047160321, 1\},$
$\{333231554619062719816252168572145127475879222724690 5$
$7938406361694282211, 1\}\}$

Observe that all the exponent of the prime factors are 1, namely they are all square-free. Thus we conclude the following:

Theorem 4.5. *The graphs Γ_k in Figure 2 are not principal graphs of subfactor for* $13 \geq k > 1$.

Note that from discriminant test it is also very likely that the theorem is true for the case $19 \geq k > 13$: the only reservation for this range is irreducibility of r_k's, as noted earlier. At this point we hope for a proof for the following conjecture:

Conjecture 4.6. *The graphs Γ_k in Figure 2 are not principal graphs of subfactor for any $k > 1$.*

References

[1] Asaeda, M. and Haagerup, U. (1999). Exotic subfactors of finite depth with Jones indices $(5+\sqrt{13})/2$ and $(5+\sqrt{17})/2$. *Communications in Mathematical Physics*, **202**, 1–63.

[2] Bion-Nadal, J. (1992). Subfactor of the hyperfinite II_1 factor with Coxeter graph E_6 as invariant. *Journal of Operator Theory*, **28**, 27–50.

[3] Bisch, D. (1998). Principal graphs of subfactors with small Jones index. *Mathematische Annalen*, **311**, 223–231.

[4] Etingof, P., Nikshych, D. and Ostrik, V. (2005) On fusion categories. *Annals of Mathematics*, **162**, 581–642.

[5] Evans, D. E. and Kawahigashi, Y. (1998). Quantum symmetries on operator algebras. *Oxford University Press.*
[6] The GAP Group. GAP Groups, Algorithms, and Programming, Version 4.4.6, 2005. (http://www.gap-system.org).
[7] Goodman, F., de la Harpe, P. and Jones, V. F. R. (1989). Coxeter graphs and towers of algebras. *MSRI Publications (Springer)*, **14**.
[8] Haagerup, U. (1994). Principal graphs of subfactors in the index range $4 < 3+\sqrt{2}$. in *Subfactors — Proceedings of the Taniguchi Symposium, Katata —*, (ed. H. Araki, et al.), World Scientific, 1–38.
[9] Haagerup, U. (2006). Private communications.
[10] Hungerford, T.W. Algebra *GTM*, **73**, Springer Verlag.
[11] Ikeda, K. (1998). Numerical evidence for flatness of Haagerup's connections. *Journal of the Mathematical Sciences, University of Tokyo*, **5**, 257–272.
[12] Izumi, M. (1991). Application of fusion rules to classification of subfactors. *Publications of the RIMS, Kyoto University*, **27**, 953–994.
[13] Izumi, M. and Kawahigashi, Y. (1993). Classification of subfactors with the principal graph $D_n^{(1)}$. *Journal of Functional Analysis*, **112**, 257–286.
[14] Izumi, M. (1994). On flatness of the Coxeter graph E_8. *Pacific Journal of Mathematics*, **166**, 305–327.
[15] Jones, V. F. R. (1983). Index for subfactors. *Inventiones Mathematicae*, **72**, 1–25.
[16] Kawahigashi, Y. (1995). On flatness of Ocneanu's connections on the Dynkin diagrams and classification of subfactors. *Journal of Functional Analysis*, **127**, 63–107.
[17] Komatsu, K. (1991) Square-free discriminants and affect-free equations. *Tokyo J. Math*,**14**, no. 1, 57–60.
[18] Kondo, T. (1995) Algebraic number fields with the discriminant equal to that of a quadratic number field. *J. Math. Soc. Japan*, **47**, 31–36.
[19] Lang, S. Algebraic Number Theory. *GTM*, **110**, Springer Verlag.
[20] Milne, J.S., Fields and Galois Theory. http://www.jmilne.org/math/CourseNotes/math594f.html
[21] Ocneanu, A. (1988). Quantized group, string algebras and Galois theory for algebras. *Operator algebras and applications, Vol. 2 (Warwick, 1987)*, (ed. D. E. Evans and M. Takesaki), London Mathematical Society Lecture Note Series Vol. 136, Cambridge University Press, 119–172.
[22] Popa, S. (1994). Classification of amenable subfactors of type II. *Acta Mathematica*, **172**, 163–255.
[23] Sunder, V. S. and Vijayarajan, A. K. (1993). On the non-occurrence of the Coxeter graphs β_{2n+1}, E_7, D_{2n+1} as principal graphs of an inclusion of II_1 factors. *Pacific Journal of Mathematics* **161**, 185–200.
[24] van der Waerden, B.L. (1949). Modern algebra (English), Frederick Ungar Publishing Co.
[25] Washington, L. (1996). Introduction to Cyclotomic Fields. *GTM*, **83**, Springer Verlag.
[26] Wenzl, H. (1988). Hecke algebras of type A_n and subfactors. *Inventiones Mathematicae*, **92**, 345–383.

Department of Mathematics, University of California Riverside, 900 Big Springs Drive, Riverside, CA, 92521 , USA
E-mail address: marta@math.ucr.edu